LOYALIST COLLEGE
IN TORONTO

Week 12 – Lab Assignment

Wireshark Lab

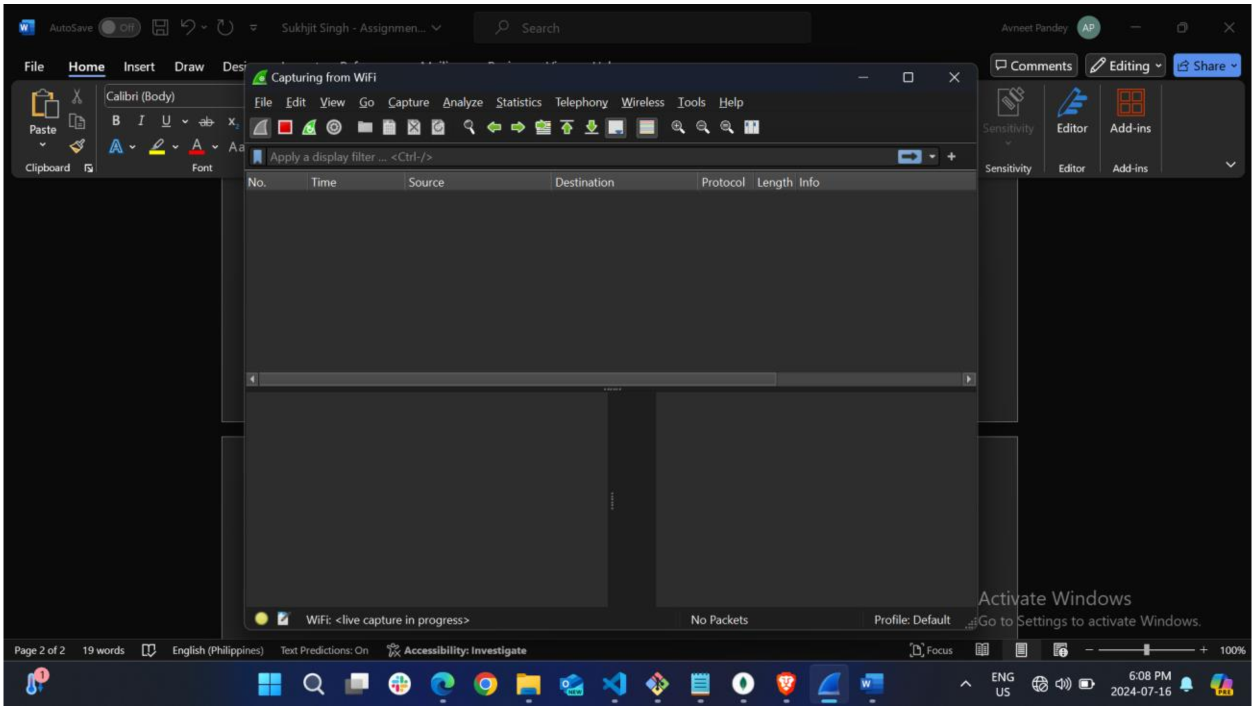
Student Name: Avneet Pandey

Student ID: 500235961

Instructor Name: Sergio Loza

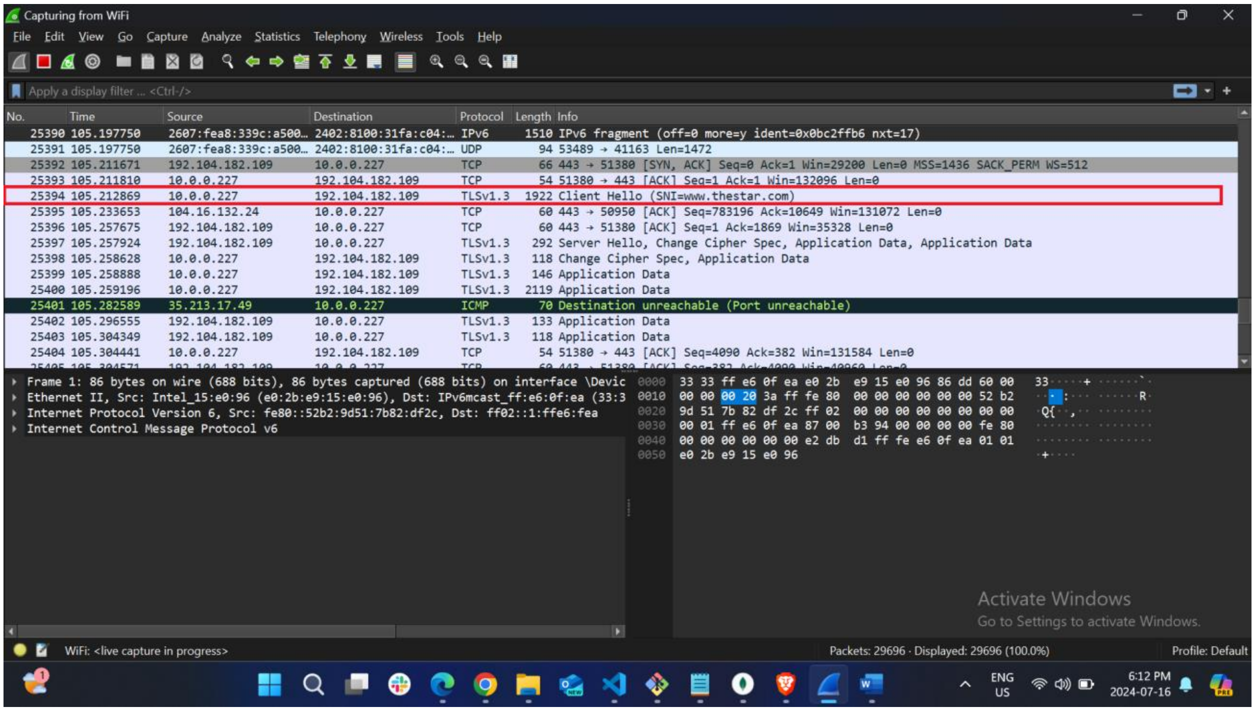
During Setup:

1) Turn Off the Wifi and the packets are stopped receiving. Therefore, clear out the screen.



Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
WiFi: <live capture in progress>
No Packets
Profile: Default
Activate Windows
Go to Settings to activate Windows.
6:08 PM
2024-07-16

2) Turn on the Wifi and hit the URL mentioned and download the file to the file system.



Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
6:12 PM
2024-07-16

```
No.   Time       Source              Destination         Protocol Length Info
25390 105.197750 2607:fea8:339c:a500… 2402:8100:31fa:c04:… IPv6   1510 IPv6 fragment (off=0 more=y ident=0x0bc2ffb6 nxt=17)
25391 105.197750 2607:fea8:339c:a500… 2402:8100:31fa:c04:… UDP      94 53489 → 41163 Len=1472
25392 105.211671 192.104.182.109     10.0.0.227          TCP        66 443 → 51380 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1436 SACK_PERM WS=512
25393 105.211810 10.0.0.227          192.104.182.109     TCP        54 51380 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
25394 105.212869 10.0.0.227          192.104.182.109     TLSv1.3  1922 Client Hello (SNI=www.thestar.com)
25395 105.233653 104.16.132.24       10.0.0.227          TCP        60 443 → 50950 [ACK] Seq=783196 Ack=10649 Win=131072 Len=0
25396 105.257675 192.104.182.109     10.0.0.227          TCP        60 443 → 51380 [ACK] Seq=1 Ack=1869 Win=35328 Len=0
25397 105.257924 192.104.182.109     10.0.0.227          TLSv1.3   292 Server Hello, Change Cipher Spec, Application Data, Application Data
25398 105.258628 10.0.0.227          192.104.182.109     TLSv1.3   118 Change Cipher Spec, Application Data
25399 105.258888 10.0.0.227          192.104.182.109     TLSv1.3   146 Application Data
25400 105.259196 10.0.0.227          192.104.182.109     TLSv1.3  2119 Application Data
25401 105.282589 35.213.17.49        10.0.0.227          ICMP       70 Destination unreachable (Port unreachable)
25402 105.296555 192.104.182.109     10.0.0.227          TLSv1.3   133 Application Data
25403 105.304349 192.104.182.109     10.0.0.227          TLSv1.3   118 Application Data
25404 105.304441 10.0.0.227          192.104.182.109     TCP        54 51380 → 443 [ACK] Seq=4090 Ack=382 Win=131584 Len=0
```

```
▸ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Devic
▸ Ethernet II, Src: Intel_15:e0:96 (e0:2b:e9:15:e0:96), Dst: IPv6mcast_ff:e6:0f:ea (33:3
▸ Internet Protocol Version 6, Src: fe80::52b2:9d51:7b82:df2c, Dst: ff02::1:ffe6:fea
▸ Internet Control Message Protocol v6
```

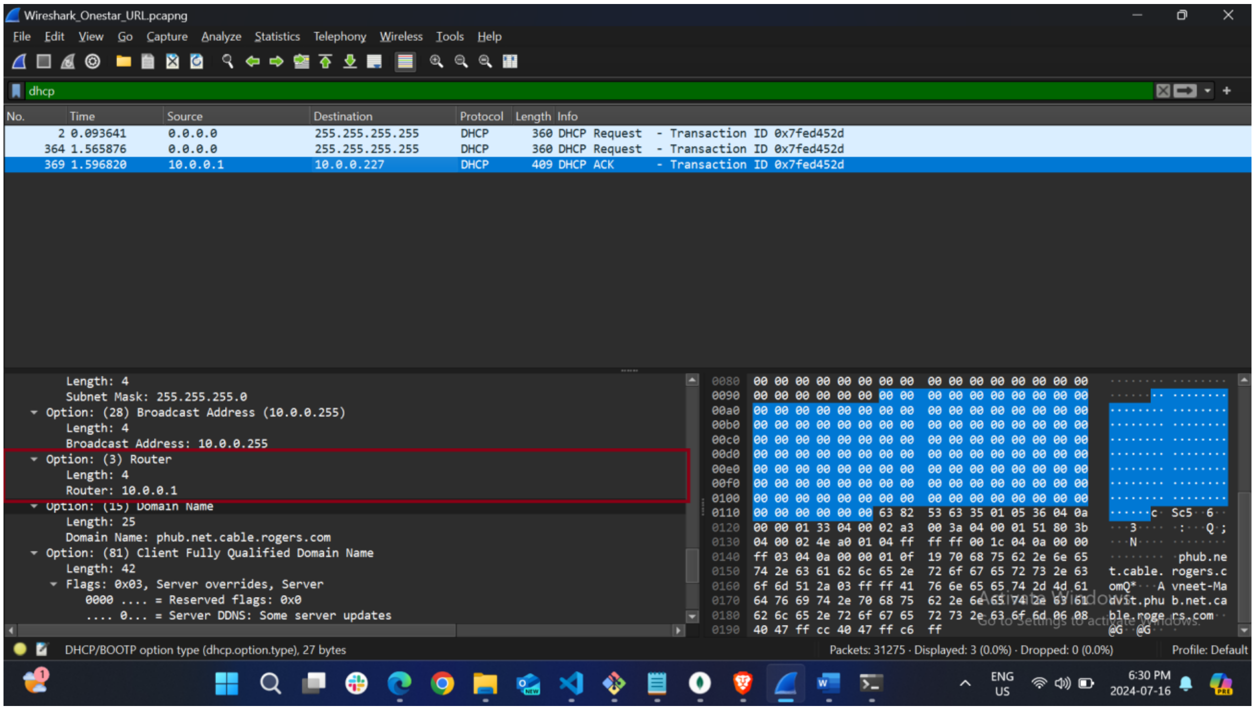
```
0000  33 33 ff e6 0f ea e0 2b  e9 15 e0 96 86 dd 60 00   33····+·······`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 52 b2   ··· :·········R·
0020  9d 51 7b 82 df 2c ff 02  00 00 00 00 00 00 00 00   ·Q{··,··········
0030  00 01 ff e6 0f ea 87 00  b3 94 00 00 00 00 fe 80   ················
0040  00 00 00 00 00 00 e2 db  d1 ff fe e6 0f ea 01 01   ················
0050  e0 2b e9 15 e0 96                                  ·+····
```

WiFi: <live capture in progress>   Packets: 29696 · Displayed: 29696 (100.0%)   Profile: Default

File Analysis:

1) Find your default router. Which IP address the default router is using? Show a screen capture with packets sent to the default router.

   Here, I’ve applied the filter of the dhcp to filter out the packets. In the accordion of the dhcp acknowledgement packet the router address is mentioned which is **10.0.0.1**


Wireshark_Onestar_URL.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time       Source      Destination       Protocol Length Info
    2 0.093641   0.0.0.0     255.255.255.255   DHCP      360 DHCP Request  - Transaction ID 0x7fed452d
  364 1.565876   0.0.0.0     255.255.255.255   DHCP      360 DHCP Request  - Transaction ID 0x7fed452d
  369 1.596820   10.0.0.1    10.0.0.227        DHCP      409 DHCP ACK      - Transaction ID 0x7fed452d
```

```
        Length: 4
        Subnet Mask: 255.255.255.0
    Option: (28) Broadcast Address (10.0.0.255)
        Length: 4
        Broadcast Address: 10.0.0.255
    Option: (3) Router
        Length: 4
        Router: 10.0.0.1
    Option: (15) Domain Name
        Length: 25
        Domain Name: phub.net.cable.rogers.com
    Option: (81) Client Fully Qualified Domain Name
        Length: 42
        Flags: 0x03, Server overrides, Server
            0000 .... = Reserved flags: 0x0
            .... 0... = Server DDNS: Some server updates
```

```
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 0a   ······c· Sc5··6··
0120  00 00 01 33 04 00 02 a3  00 3a 04 00 01 51 80 3b   ···3···· ·:···Q·;
0130  04 00 02 4e a0 01 04 ff  ff ff 00 1c 04 0a 00 00   ···N···· ········
0140  ff 03 04 0a 00 00 01 0f  19 70 68 75 62 2e 6e 65   ········ ·phub.ne
0150  74 2e 63 61 62 6c 65 2e  72 6f 67 65 72 73 2e 63   t.cable. rogers.c
0160  6f 6d 51 2a 03 ff ff 41  76 6e 65 65 74 2d 4d 61   omQ*···A vneet-Ma
0170  64 76 69 74 2e 70 68 75  62 2e 6e 65 74 2e 63 61   dvit.phu b.net.ca
0180  62 6c 65 2e 72 6f 67 65  72 73 2e 63 6f 6d 06 08   ble.roge rs.com··
0190  40 47 ff cc 40 47 ff c6  ff                        @G··@G··
```

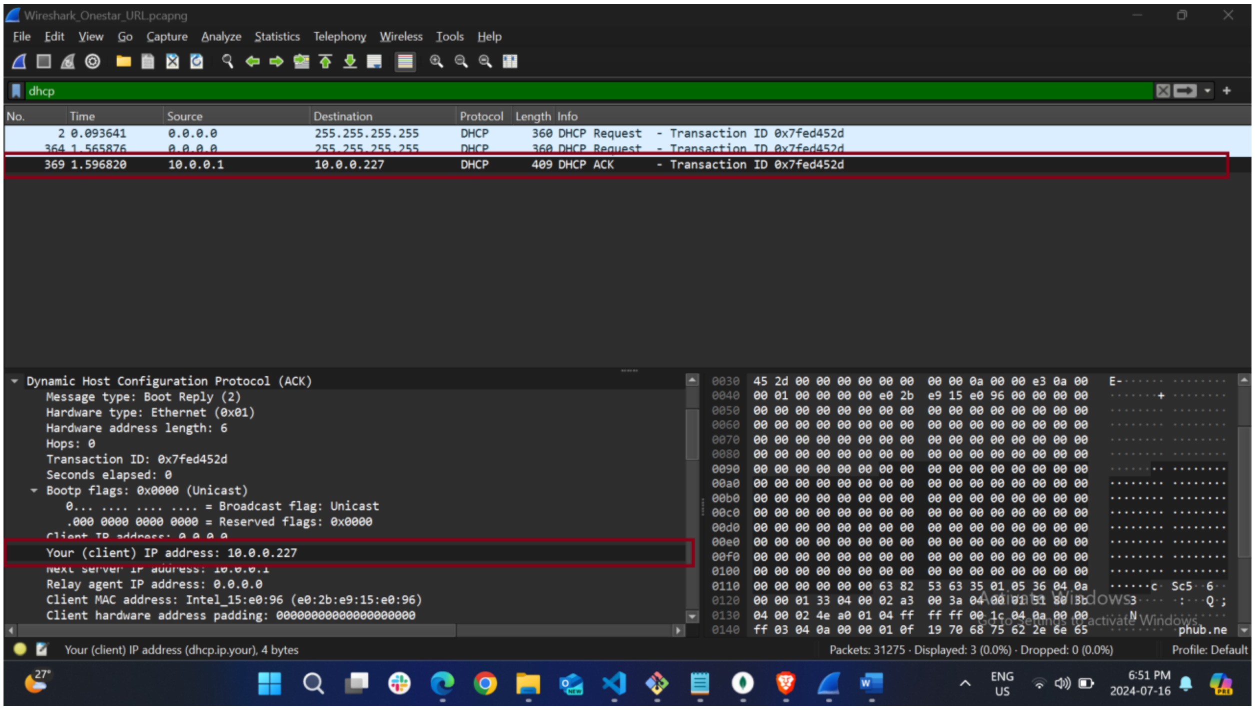
DHCP/BOOTP option type (dhcp.option.type), 27 bytes

Packets: 31275 · Displayed: 3 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

2) What is the IP address your computer is using on the wifi/ethernet adapter? Show a screen capture to support your answer.

   In the same dhcp acknowledgement package, Your client IP address is mentioned as highlighted in the below screenshot. DHCP is using **10.0.0.227** address of my PC to talk to the router.



```
dhcp
No.   Time        Source      Destination       Protocol Length Info
    2 0.093641    0.0.0.0     255.255.255.255   DHCP     360 DHCP Request  - Transaction ID 0x7fed452d
  364 1.565876    0.0.0.0     255.255.255.255   DHCP     360 DHCP Request  - Transaction ID 0x7fed452d
  369 1.596820    10.0.0.1    10.0.0.227        DHCP     409 DHCP ACK      - Transaction ID 0x7fed452d
```

```
Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7fed452d
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.0.0.227
    Next server IP address: 10.0.0.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: Intel_15:e0:96 (e0:2b:e9:15:e0:96)
    Client hardware address padding: 00000000000000000000
```

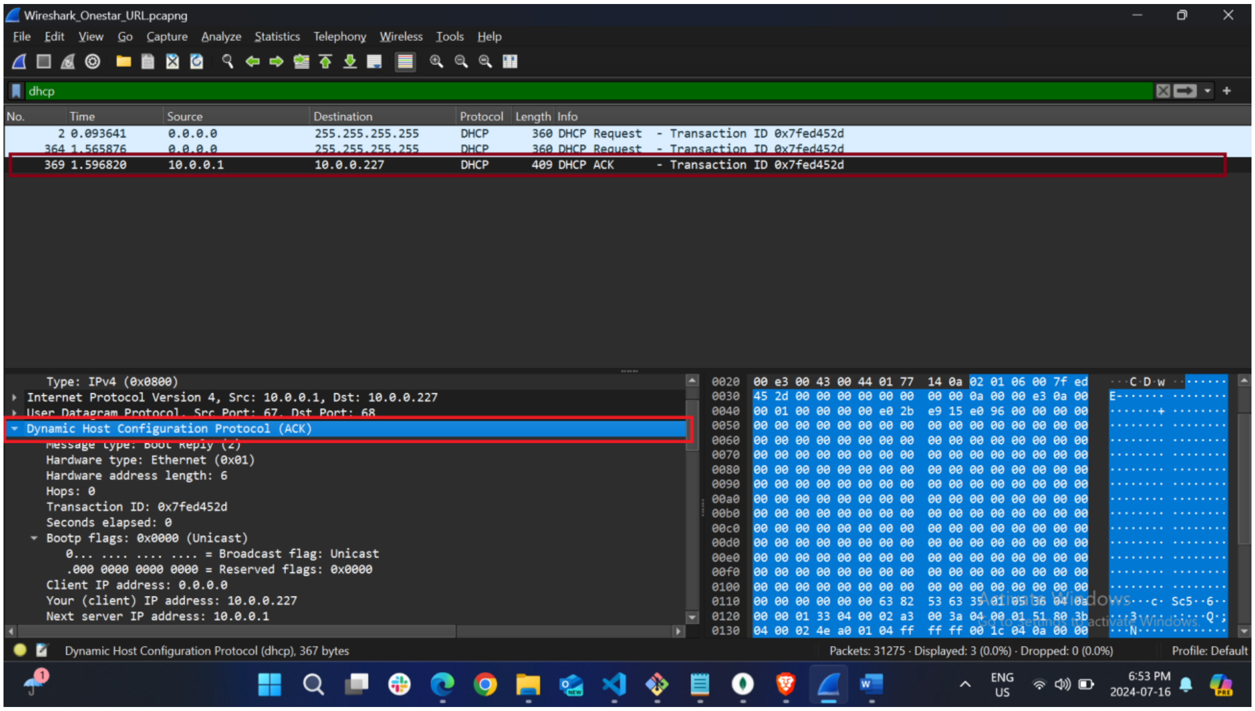
```
0030  45 2d 00 00 00 00 00 00  00 00 0a 00 00 e3 0a 00
0040  00 01 00 00 00 00 e0 2b  e9 15 e0 96 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 0a
0120  00 00 01 33 04 00 02 a3  00 3a 04 00 01 51 80 3b
0130  04 00 02 4e a0 01 04 ff  ff ff 00 1c 04 0a 00 00
0140  ff 03 04 0a 00 00 01 0f  19 70 68 75 62 2e 6e 65   phub.ne
```

Your (client) IP address (dhcp.ip.your), 4 bytes · Packets: 31275 · Displayed: 3 (0.0%) · Dropped: 0 (0.0%) · Profile: Default

Wireshark_Onestar_URL.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
27°
ENG
US
6:51 PM
2024-07-16

3) What is the protocol used to obtain your IP Address? Show the screen capture with this protocol.

DHCP: Dynamic Host Configuration protocol is used to find the IP address our PC as it is responsible for the automatically allocate the IP address. Due to this we are able to find the answer of the above questions.



```
dhcp
No.   Time        Source      Destination       Protocol Length Info
    2 0.093641    0.0.0.0     255.255.255.255   DHCP     360 DHCP Request  - Transaction ID 0x7fed452d
  364 1.565876    0.0.0.0     255.255.255.255   DHCP     360 DHCP Request  - Transaction ID 0x7fed452d
  369 1.596820    10.0.0.1    10.0.0.227        DHCP     409 DHCP ACK      - Transaction ID 0x7fed452d
```

```
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.227
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7fed452d
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.0.0.227
    Next server IP address: 10.0.0.1
```

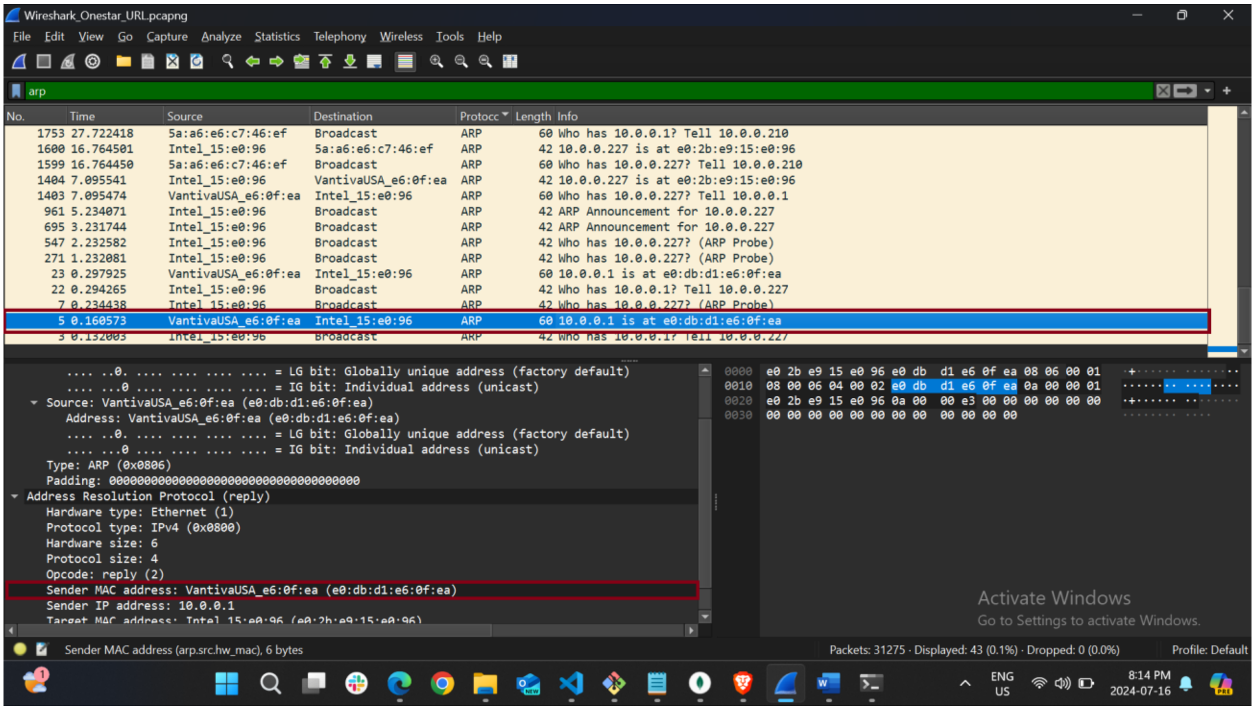
```
0020  00 e3 00 43 00 44 01 77  14 0a 02 01 06 00 7f ed   ···C·D·w ········
0030  45 2d 00 00 00 00 00 00  00 00 0a 00 00 e3 0a 00
0040  00 01 00 00 00 00 e0 2b  e9 15 e0 96 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 0a
0120  00 00 01 33 04 00 02 a3  00 3a 04 00 01 51 80 3b
0130  04 00 02 4e a0 01 04 ff  ff ff 00 1c 04 0a 00 00
```

Dynamic Host Configuration Protocol (dhcp), 367 bytes · Packets: 31275 · Displayed: 3 (0.0%) · Dropped: 0 (0.0%) · Profile: Default

Wireshark_Onestar_URL.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ENG
US
6:53 PM
2024-07-16

4) What is the protocol that is used to find the MAC address of the default router? What is the MAC address of the default router? Show a screenshot with this protocol.

Address Resolution Protocol (ARP) is used to find the MAC address of the default router. Therefore, to find the MAC address of the default router I've put the filter of arp. Remember, we found the address of the default router in 1st step, we can use it to find the mac address of that particular IP address. We will search for broadcast message of ARP "who has 10.0.0.1" Then search for the response of that IP address which will eventually gives the mac address of the device i.e. **e0:db:d1:e6:0f:ea**


Wireshark_Onestar_URL.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Activate Windows
Go to Settings to activate Windows.
ENG
US
8:14 PM
2024-07-16

arp

```
No.   Time      Source               Destination          Protocc  Length Info
 1753 27.722418 5a:a6:e6:c7:46:ef    Broadcast            ARP      60 Who has 10.0.0.1? Tell 10.0.0.210
 1600 16.764501 Intel_15:e0:96       5a:a6:e6:c7:46:ef    ARP      42 10.0.0.227 is at e0:2b:e9:15:e0:96
 1599 16.764450 5a:a6:e6:c7:46:ef    Broadcast            ARP      60 Who has 10.0.0.227? Tell 10.0.0.210
 1404 7.095541  Intel_15:e0:96       VantivaUSA_e6:0f:ea  ARP      42 10.0.0.227 is at e0:2b:e9:15:e0:96
 1403 7.095474  VantivaUSA_e6:0f:ea  Intel_15:e0:96       ARP      60 Who has 10.0.0.227? Tell 10.0.0.1
  961 5.234071  Intel_15:e0:96       Broadcast            ARP      42 ARP Announcement for 10.0.0.227
  695 3.231744  Intel_15:e0:96       Broadcast            ARP      42 ARP Announcement for 10.0.0.227
  547 2.232582  Intel_15:e0:96       Broadcast            ARP      42 Who has 10.0.0.227? (ARP Probe)
  271 1.232081  Intel_15:e0:96       Broadcast            ARP      42 Who has 10.0.0.227? (ARP Probe)
   23 0.297925  VantivaUSA_e6:0f:ea  Intel_15:e0:96       ARP      60 10.0.0.1 is at e0:db:d1:e6:0f:ea
   22 0.294265  Intel_15:e0:96       Broadcast            ARP      42 Who has 10.0.0.1? Tell 10.0.0.227
    7 0.234438  Intel_15:e0:96       Broadcast            ARP      42 Who has 10.0.0.227? (ARP Probe)
    5 0.160573  VantivaUSA_e6:0f:ea  Intel_15:e0:96       ARP      60 10.0.0.1 is at e0:db:d1:e6:0f:ea
    3 0.132003  Intel_15:e0:96       Broadcast            ARP      42 Who has 10.0.0.1? Tell 10.0.0.227
```

```
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: VantivaUSA_e6:0f:ea (e0:db:d1:e6:0f:ea)
        Address: VantivaUSA_e6:0f:ea (e0:db:d1:e6:0f:ea)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: VantivaUSA_e6:0f:ea (e0:db:d1:e6:0f:ea)
    Sender IP address: 10.0.0.1
    Target MAC address: Intel_15:e0:96 (e0:2b:e9:15:e0:96)
```

```
0000  e0 2b e9 15 e0 96 e0 db  d1 e6 0f ea 08 06 00 01
0010  08 00 06 04 00 02 e0 db  d1 e6 0f ea 0a 00 00 01
0020  e0 2b e9 15 e0 96 0a 00  00 e3 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

Sender MAC address (arp.src.hw_mac), 6 bytes

Packets: 31275 · Displayed: 43 (0.1%) · Dropped: 0 (0.0%)

Profile: Default